UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/222,846	12/30/1998	KAZUOMI OISHI	35.G2331	2585

5514 7590 05/04/2004

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
MEISLAHN, DOUGLAS J	
ART UNIT	**PAPER NUMBER**
2137	22

DATE MAILED: 05/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/222,846	OISHI, KAZUOMI	
	Examiner	Art Unit	
	Douglas J. Meislahn	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,6,7,10-14,18-20 and 22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 6, 7, 10-14, 18-20, and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the request for reconsideration filed 20 February 2004. Applicant's arguments have overcome the 112 rejection.

Response to Arguments

2. Applicant's arguments filed 20 February 2004 have been fully considered but they are not persuasive.

3. Applicant's interpretation of "immediately", that being sufficiently close in time to the completion of encryption and before outputting encrypted data, encompasses the examiner's understanding of Ryan, Jr. et al. It is unclear how applicant is differentiating their interpretation of "immediately" from Ryan, Jr. et al.

4. Applicant does argue that Ryan, Jr. et al. transmit data prior to erasing the key, basing this line of reasoning on the erasure occurring after the completion of the requested function. Applicant says that the requested function results in the encryption and transmission of data. Applicant provides no evidence of the validity of this interpretation of Ryan, Jr. et al. Applicant's analysis is flawed because, as stated in lines 27-29 of column 4 of the patent in question, the key is used to perform a requested function. Keys are not used to transmit data. As such, transmitting data is not the requested function. Furthermore, in lines 60-67 of column 3, encryption, among other things, is listed as a potential function.

5. Part of applicant's confusion might stem from the author of Ryan, Jr. et al.'s patent horribly misrepresenting the system. In the cited section, the author

says that K_{KMS} is used to decrypt encrypted keys, and then that same K_{KMS} is used to perform the function, following which the plaintext copy is decrypted, but an encrypted version of K_{KMS} still remains in the database that contains the encrypted keys. Ryan, Jr. et al. would not decrypt encrypted keys with K_{KMS} only to continue to use K_{KMS}. The decrypted keys are actually the ones that are used to perform the functions. They are subsequently erased, although an encrypted copy remains in the database.

6. Applicant argues that this remaining encrypted copy differentiates the claims from Ryan, Jr. et al. This line of thought is incorrect. First, at no point do the claims preclude maintaining an encrypted form of the key. They only stipulate that a copy of the key be erased. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the erasure of all copies of a key) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Also, the encrypted database in Ryan, Jr. et al. is external to the entity that decrypts the keys; requiring the erasure of this database would be similar to requiring that the external source in applicant's claims erase its copies of the key.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 3, 6, 10, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hickman et al. (5619025) in view of Ryan, Jr. et al. (6192473).

In the first paragraph of column 5, Hickman et al. show the use of image data as an encryption key. As detailed in their previous paragraph, this image data is collected from a document. The document reads on applicant's external source, while collection of data mandates reading means. Use of the image as an encryption key requires storage of the encryption key and encryption means to perform the actual encryption. The encrypted data is sent to an electronic database, which necessitates output means. Hickman et al. do not require the encryption key to be erased before the encrypted material is transmitted. In lines 29-35 of column 4, Ryan, Jr. et al. teach improving security by erasing encryption keys "[i]mmediately" after their use. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to improve security by erasing the encryption keys used in Hickman et al., as taught by Ryan, Jr. et al.

9. Claims 2 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hickman et al. in view of Ryan, Jr. et al. (6192473) as applied to claims 1 and 10 above.

Hickman et al. and Ryan, Jr. et al. show a key being read from an external source, used to encrypt a document, and deleted upon transmittal of the encrypted document. They do not say that the encrypted data had undergone a high-efficiency coding operation prior to encryption. Official notice is taken that it is old and well-known to subject data to high-efficiency coding operations as a way to reduce the size of the data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to subject the to-be-encrypted data in Hickman et al. to a high-efficiency coding operation in order to reduce the amount of raw data that needs to be encrypted and transmitted.

10. Claims 7, 18-20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hickman et al. in view of Ryan, Jr. et al. (6192473) as applied to claim 1 above and further in view of Schneier (*Applied Cryptography*).

Hickman et al. and Ryan, Jr. et al. show a key being read from an external source, used to encrypt a document, and deleted upon encryption of the document. With respect to claim 7, they do not say that the encryption key is based on a public key cryptosystem. On page 48, Schneier teaches encrypting messages with a key based on a public key cryptosystem. This system allows anyone to have the power to encrypt, but only one entity to have the power to decrypt. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for the encryption key in Hickman et al. to be a public key so that either only one entity could decrypt encrypted message or only one entity could have encrypted (by decryption) the message.

With respect to claims 18-20 and 22, they do not say that the document is actually encrypted by a second key while the key read from the external source is used to encrypt the second key. On page 176, Schneier teaches key-encryption keys and mentions that they should be distributed manually. On page 184, Schneier talks about how key-encryption keys are seldom distributed and are used to generate little ciphertext. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the keys on Hickman et al.'s external source as a key-encryption key, thus generating a minimal amount of ciphertext with the key, which reduces the benefit of replacing the key. Thus, the external source would have a longer feasible lifetime. With respect to claim 19, Schneier teaches encrypting a symmetric key with a recipient's public key on page 51; that is, the key-encryption key is from a public-key cryptosystem.

11. Claims 1, 6, 10, 13, and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laing et al. (5534857) in view of Ryan, Jr. et al. (6192473).

In lines 18-20 of column 9, Laing et al. disclose enciphering a random number with a key that has been read from a smart card. The smart card is an external source. Reading means are inherent for the reading step. As such the first clause of claim 1 is rendered obvious. Storage means for the encryption key are inherent because the key must be stored in order to be used. Thus, the second clause of the first claim is met. In lines 21-23 of the same column, the encrypted random number is transmitted, which renders obvious output means and the third clause of claim 1. Laing et al. do not require the encryption key to

be erased before the encrypted material is transmitted. In lines 29-35 of column 4, Ryan, Jr. et al. teach improving security by erasing encryption keys "[i]mmediately" after their use. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to improve security by erasing the encryption keys used to encrypt the random number in Laing et al., as taught by Ryan, Jr. et al.

Claims 6 and 13 are rendered obvious by lines 24-35 of column 9 in Laing et al. Claim 10 is rendered obvious because it is a method for the means of claim 1 and claim 14 because it is a computer readable medium with instructions for performing the steps of claim 10.

12. Claims 2 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laing et al. in view of Ryan, Jr. et al. (6192473).

Laing et al. and Ryan, Jr. et al. show a key being read from a smart card and being used to encrypt a random number. They do not say that the encrypted data had undergone a high-efficiency coding operation prior to encryption. Official notice is taken that it is old and well-known to subject data to high-efficiency coding operations as a way to reduce the size of the data. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to subject the to-be-encrypted data in Laing et al. to a high-efficiency coding operation in order to reduce the amount of raw data that needs to be encrypted and transmitted.

13. Claims 3 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laing et al. in view of Ryan, Jr. et al. as applied to claims 1 and 10 above.

Laing et al. and Ryan, Jr. et al. show a key being read from a smart card and being used to encrypt a random number. They do not say that a scanner is attached to their system. Official notice is taken that it is old and well-known to attach scanners to computer systems, thereby letting the system scan documents and pictures. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to add a scanner to the system of Laing et al. and Ryan, Jr. et al.

14. Claims 7, 18-20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laing et al. in view of Ryan, Jr. et al. (6192473) as applied to claim 1 above and further in view of Schneier (*Applied Cryptography*).

Laing et al. and Ryan, Jr. et al. show a key being read from a smart card and being used to encrypt a random number. With respect to claim 7, they do not say that the encryption key is based on a public key cryptosystem. On page 48, Schneier teaches encrypting messages with a key based on a public key cryptosystem. This system allows anyone to have the power to encrypt, but only one entity to have the power to decrypt. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made for the encryption key in Laing et al. to be a public key so that either only one entity could decrypt encrypted message or only one entity could have encrypted (by decryption) the message.

With respect to claims 18-20 and 22, they do not say that the random number is actually encrypted by a second key while the key read from the external source is used to encrypt the second key. On page 176, Schneier teaches key-encryption keys and mentions that they should be distributed manually. On page 184, Schneier talks about how key-encryption keys are seldom distributed and are used to generate little ciphertext. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to use the key on Laing et al.'s smart card as a key-encryption key, thus generating a minimal amount of ciphertext with the key, which reduces the benefit of replacing the key. Thus, the external source would have a longer feasible lifetime. With respect to claim 19, Schneier teaches encrypting a symmetric key with a recipient's public key on page 51; that is, the key-encryption key is from a public-key cryptosystem.

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

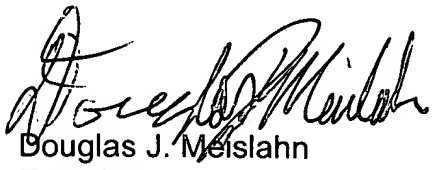
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Douglas J. Meislahn
Examiner
Art Unit 2137

DJM